Séminaire Lotharingien de Combinatoire **54A** (2006), Article B54Ap

A GENERALIZATION OF COBHAM'S THEOREM FOR REGULAR SEQUENCES

Jason P. Bell*

Department of Mathematics, Simon Fraser University
8888 University Ave., Burnaby, BC V5A 1S6, Canada
jpb@math.sfu.ca

Abstract. A sequence is said to be k-*automatic* if the n^{th} term of this sequence is generated by a finite state machine with n in base k as input. A result due to Cobham states that if a sequence is both k- and ℓ-automatic and k and ℓ are multiplicatively independent, then the sequence is eventually periodic. Allouche and Shallit defined (R, k)-regular sequences as a natural generalization of k-automatic sequences for a given ring R. In this paper we prove the following generalization of Cobham's theorem: If a sequence is (R, k)- and (R, ℓ)-regular and k and ℓ are multiplicatively independent, then the sequence satisfies a linear recurrence over R.

1. Introduction

Given a positive integer k, a sequence is said to be k-*automatic* if the n^{th} term of this sequence is generated by a finite state machine with n in base k as input. Sequences such as the Thue-Morse and Rudin-Shapiro sequences are famous examples of 2-automatic sequences. Automatic sequences appear in many diverse areas of mathematics including an unexpected appearance in paper folding [7], [8], [9].

Arguably the most important theorem in the theory of automatic sequences is Cobham's theorem. This theorem characterizes sequences that are both k- and ℓ-automatic when k and ℓ are *multiplicatively independent* integers; that is, when there do not exist positive integers a and b such that $k^a = \ell^b$.

Theorem 1.1 (Cobham [6]). *Let k and ℓ be multiplicatively independent integers and let $\{f(n)\}$ be a sequence which is both k- and ℓ-automatic. Then $\{f(n)\}$ is eventually periodic.*

* Supported in part by the by the National Science Foundation under Grant No. DMS-0502858.

Over the years many different proofs and some generalizations of his theorem have been given [17], [18], [20], [24], [15], [11], [21], [19], [12]. To give our generalization of Cobham's theorem, we need a generalization of automatic sequences due to Allouche and Shallit [1], [2], [3].

Another way of defining the k-automatic property comes from looking at the k-*kernel* of a sequence. The k-kernel of a sequence $\{f(n)\}_{n=0}^{\infty}$ is defined to be the collection of sequences of the form $\{f(k^i n+j)\}_{n=0}^{\infty}$ where $i \geq 0$ and $0 \leq j < k^i$. A sequence is k-automatic if and only if its k-kernel is finite. Using this definition of k-automatic sequences, Allouche and Shallit [1], [2], [3] generalized the notion of being k-automatic. We note that this concept is very closely related to the more general notion of recognizable series [5].

Let R be a commutative ring. Given a sequence $\{f(n)\}_{n=0}^{\infty}$ taking values in some R-module, we create an R-module $M_R(\{f(n)\}; k)$ which is defined to be the R-module generated by all sequences $\{f(k^i n+j)\}_{n=0}^{\infty}$, where $i \geq 0$ and $0 \leq j < k^i$. Often, we will suppress the R in $M_R(\{f(n)\}; k)$ and just write $M(\{f(n)\}; k)$ when there is no fear of confusion.

Definition 1.2. Let R be a commutative ring and let k be a positive integer. A sequence is (R, k)-*regular* if $M(\{f(n)\}; k)$ is finitely generated as an R-module.

In fact, Allouche and Shallit impose the additional constraint that the ground ring R be Noetherian when looking at (R, k)-regular sequences, but this hypothesis is not necessary in obtaining our generalization.

Since the k-kernel of a sequence $\{f(n)\}$ spans $M(\{f(n)\}; k)$ as an R-module, we see that a k-automatic sequence with values in R is necessarily (R, k)-regular for any ring R.

Unlike automatic sequences, which only assume finitely many values, regular sequences can assume infinitely many values. For this reason it is unrealistic to assume that the correct analogue of Cobham's theorem for regular sequences is that an (R, k)- and (R, ℓ)-regular sequence is eventually periodic if k and ℓ are multiplicatively independent. There is, however, a larger class of sequences which gives the correct analogue.

Definition 1.3. Given a commutative ring R and R-module M, we say that a map

$$f : \mathbb{N} \to M$$

satisfies a linear recurrence over R, if there exist a positive integer m and constants $c_1, \ldots, c_m \in R$ such that

$$f(n) \ = \ \sum_{i=1}^{m} c_i f(n-i) \qquad \text{for } n \geq m.$$

If $\{f(n)\}$ satisfies a linear recurrence over a ring R and assumes only finitely many values, then $\{f(n)\}$ is eventually periodic (cf. Everest et al. [14, §3.1]). Furthermore, given an eventually periodic sequence $\{f(n)\}$ there exist numbers m and N such that $\{f(n)\}$ satisfies the linear recurrence $f(n+m) = f(n)$ for $n \geq N$. Our main result is the following theorem.

Theorem 1.4 (Generalized Cobham Theorem). *Let R be a commutative ring, let k and ℓ be multiplicatively independent positive integers, and let $\{f(n)\}$ be a sequence which is both (R,k)- and (R,ℓ)-regular. Then $\{f(n)\}$ satisfies a linear recurrence over R.*

In light of the above remarks, this is indeed a generalization of Cobham's theorem. In the case that $R = \mathbb{Z}$, an (R,k)-regular sequence is called k-regular. In this case we get a simple characterization of sequences which are both k- and ℓ-regular if k and ℓ are multiplicatively independent.

Theorem 1.5. *Let $\{f(n)\}$ be an integer valued sequence and let k and ℓ be two multiplicatively independent positive integers. Then $\{f(n)\}$ is both k- and ℓ-regular if and only if*

$$\sum_{n=0}^{\infty} f(n)x^n \in \mathbb{Z}[[x]]$$

is the power series expansion of a rational function whose poles are all roots of unity.

Our proof of Theorem 1.4 is ring-theoretic in nature, using a series of reductions. The argument is first done for the case that the ring R is a finitely generated integral domain over $\mathbb{Z}$ and the sequence $\{f(n)\}$ takes values in R. To do this we need some basic facts about such rings; namely, that all maximal ideals have finite codimension and that the intersection of all maximal ideals is (0). Next the general version of the theorem is deduced by showing one can assume that R is a finitely generated algebra over $\mathbb{Z}$; then, we show that R can also be assumed to be an integral domain. Finally, using similar arguments applied to R-modules, we show that one can assume that $\{f(n)\}$ takes values in R. Having reduced everything to the case we have already handled, we obtain our generalization of Cobham's theorem.

In §2, we give some basic background in the theory of commutative rings. In §3 we prove Theorem 1.4 for finitely generated integral domains R over $\mathbb{Z}$ with R-valued sequences. In §4 we reduce the problem to the case handled in §3. Finally in §5 we give an open problem along with some concluding remarks.

2. Background in commutative rings

Jacobson rings form an important class of rings and are especially useful in formulating the general Nullstellensatz. We now give the definition of a Jacobson ring, first recalling that an ideal in a ring is *prime* if when we quotient out by this ideal we obtain a integral domain.

Definition 2.1. We say that a commutative ring R is a *Jacobson ring* if every prime ideal is the intersection of maximal ideals.

Notice that the ring of integers is a Jacobson ring.

Theorem 2.2. *If R is a Jacobson ring and S is a finitely generated R-algebra, then S is also a Jacobson ring and every maximal ideal I in S has the property that $J := I \cap R$ is a maximal ideal of R; moveover, S/I is a finite extension of R/J.*

Proof. See Eisenbud [13, Theorem 4.19]. ☐

Corollary 2.3. *Let R be a finitely generated integral domain over $\mathbb{Z}$. Then:*

- (0) *is the intersection of maximal ideals;*
- R/I *is finite dimensional for every maximal ideal I of R.*

Proof. A finitely generated $\mathbb{Z}$-algebra is Jacobson by Theorem 2.2. If R is a integral domain then (0) is a prime ideal and thus is the intersection of maximal ideals. If I is a maximal ideal in R, then $I \cap \mathbb{Z} = (p)$ for some prime $p \in \mathbb{Z}$. Then R/I is a finite extension of $\mathbb{Z}/p\mathbb{Z}$ and is thus a finite ring. ☐

For us, the important facts about finitely generated integral domains over $\mathbb{Z}$ are those given in Corollary 2.3 are the fact that such rings are *Noetherian*; that is, they satisfy the ascending chain condition on ideals. This ensures that finitely generated modules over such rings satisfy the ascending chain condition on submodules. In particular, we can pick ideals that are maximal with respect to some specified property and can pick submodules in a finitely generated module that are maximal with respect to some property. The fact that in a finitely generated integral domain R over $\mathbb{Z}$ all maximal ideals have finite codimension has important consequences for (R, k)-regular sequences, as is seen in the following theorem.

Theorem 2.4. *Let R be a Jacobson ring and let $\{f(n)\}$ be an (R, k)-regular sequence. If I is a maximal ideal in R then $\{f(n) \bmod I\}$ is a k-automatic sequence.*

Proof. Notice that R/I is a finite field and $\{f(n)\}$ takes values in a finite dimensional R/I-vector space. It follows that $\{f(n) \bmod I\}$ takes on only finitely many values and thus is k-automatic (cf. Allouche and Shallit [3, Theorem 16.1.5]). □

3. Proofs for integral domains

In this section, we prove Theorem 1.4 in the case that R is a finitely generated integral domain over $\mathbb{Z}$ and $\{f(n)\}$ is R-valued. We first give a few basic results about rational sequences.

Lemma 3.1. *Let $\{f(n)\}$ be an integer sequence and let a be a positive integer. Then:*

- *$\{f(n)\}$ satisfies a linear recurrence if and only if $\{f(an+j)\}$ satisfies a linear recurrence for $0 \le j < a$;*
- *$\{f(n)\}$ satisfies a linear recurrence if and only if $\{f(n+a)\}$ satisfies a linear recurrence; and*
- *$\{f(n)\}$ satisfies a linear recurrence over a ring R if and only if the R-module spanned by the sequences $\{f(n+i)\}$ with $i \ge 0$ is finite dimensional.*

Proof. The proofs of these facts are straightforward. □

Lemma 3.2. *Let R be a Noetherian integral domain with field of fractions K. If $\{f(n)\}$ is an R-valued sequence satisfying a linear recurrence over K, then $\{f(n)\}$ satisfies a linear recurrence over R.*

Proof. By assumption there exist $c_1, \ldots, c_m \in K$ such that

$$f(n) \;=\; \sum_{i=1}^{m} c_i f(n-i) \qquad \text{for } n \ge m.$$

We define R^m to be the set of all m-dimensional column vectors with entries in R. For each $n \ge 0$, define

$$\mathbf{v}(n) \;=\; \begin{bmatrix} f(n) & f(n+1) & \cdots & f(n+m-1) \end{bmatrix}^{\mathrm{T}} \;\in\; R^m.$$

Then there is an $m \times m$ matrix B with entries in K such that $B\mathbf{v}(n) = \mathbf{v}(n+1)$ for all $n \ge 0$. Let M denote the R-submodule of R^m spanned by the vectors $\mathbf{v}(n)$ for $n \ge 0$. Since R is Noetherian, M is finitely generated. Hence there exists some d such that the set $\{\mathbf{v}(i) \mid 0 \le i \le d\}$ spans M as an R-module. It follows that there exist $r_0, \ldots, r_d \in R$ such that

$$\mathbf{v}(d+1) \;=\; \sum_{i=0}^{d} r_i \mathbf{v}(i).$$

Left multiplying both sides by B^n, we see that

$$\mathbf{v}(n+d+1) \;=\; \sum_{i=0}^{d} r_i \mathbf{v}(n+i) \qquad \text{for } n \geq 0.$$

Taking the first coordinates of both sides we obtain the R-linear recurrence

$$f(n+d+1) \;=\; \sum_{i=0}^{d} r_i f(n+i) \qquad \text{for } n \geq 0.$$

This completes the proof. □

Lemma 3.3. *Let R be an integral domain with field of fractions K, let k be a positive integer, and let $\{f(n)\}$ be an R-valued (R,k)-regular sequence. Suppose that $\{g(n)\}$ is an R-valued sequence such that there is an infinite set $\mathcal{M}$ of maximal ideals of R with the following properties:*

- $\bigcap_{I\in\mathcal{M}} I \;=\; (0)$;
- *for every ideal $I \in \mathcal{M}$ there exists some some sequence $h_I \in M(\{f(n)\};k)$ with the property that $g(n) \equiv h_I(n) \bmod I$ for all $n \geq 0$.*

Then $\{g(n)\} \in M(\{f(n)\};k) \otimes_R K$.

Proof. Let $I \in \mathcal{M}$ and let $f_1(n),\ldots,f_d(n)$ be a basis for $M(\{f(n)\};k)\otimes_R K$ as a K-vector space. By assumption, there exist $C_1,\ldots,C_d \in R$ such that

$$g(n) \equiv C_1 f_1(n) + \cdots + C_d f_d(n) \bmod I$$

for all $n \geq 0$. This says that every $(d+1)\times(d+1)$ minor of the infinite matrix

$$\begin{pmatrix} f_1(0) & f_1(1) & f_1(2) & \cdots \\ f_2(0) & f_2(1) & f_2(2) & \cdots \\ \vdots & \vdots & \vdots & \cdots \\ f_d(0) & f_d(1) & f_d(2) & \cdots \\ g(0) & g(1) & g(2) & \cdots \end{pmatrix}$$

is in I. Since the intersection of all ideals in $\mathcal{M}$ is zero, we conclude that every $(d+1)\times(d+1)$ minor is 0. It is well-known that a matrix with entries in some field has rank $\geq m$ if and only if some $m\times m$ minor is nonzero. It follows that the sequences $f_1,\ldots,f_d,g$ are linearly dependent over K. Since $f_1,\ldots,f_d$ are linearly independent, we conclude that g is a K-linear combination of $f_1,\ldots,f_d$. The result follows. □

We now give a criterion which allows us to deduce when certain (R,k)-regular sequences satisfy a linear recurrence over R.

Theorem 3.4. *Let R be an integral domain, let k be a positive integer, and let $\{f(n)\}$ be an R-valued (R,k)-regular sequence with the property that $\{f(n) \bmod I\}$ is periodic with period relatively prime to k for an infinite set of maximal ideals I whose intersection is (0). Then $\{f(n)\}$ satisfies a linear recurrence R.*

Proof. Let K be the field of fractions of R and let $\mathcal{M}$ be the set of maximal ideals I such that $\{f(n) \bmod I\}$ is a periodic sequence with period relatively prime to k. Let $I \in \mathcal{M}$ and let e denote the period of $\{f(n) \bmod I\}$. Since k is relatively prime to e, there exists some $a > 0$ such that $k^a \equiv 1 \bmod e$. Hence $f(k^a n + 1) \equiv f(n+1) \bmod I$ for all $n \geq 0$. It follows that for each ideal I in $\mathcal{M}$, there exists some sequence $h_I \in M(\{f(n)\}, k)$ such that $f(n+1) \equiv h_I(n) \bmod I$ for all $n \geq 0$. From Lemma 3.3, we deduce that $\{f(n+1)\} \in M(\{f(n)\}; k) \otimes_R K$. An easy induction argument shows that $\{f(n+i)\} \in M(\{f(n)\}; k) \otimes_R K$ for all $i \geq 0$. Since $M(\{f(n)\}; k) \otimes_R K$ is finite dimensional over K we see that the subspace generated by

$$\{\{f(n+i)\} \mid i \geq 0\}$$

is finite dimensional. Hence $f(n)$ satisfies a linear recurrence over K. The result now follows from Lemma 3.2 □

Definition 3.5. Given an eventually periodic sequence $\{f(n)\}$, we define the *index* of $\{f(n)\}$ to be the minimal i such that the sequence $\{f(n+i)\}_{n\geq 0}$ is periodic. We define the *minimal period* of a periodic sequence $\{f(n)\}$ to be the smallest positive integer e such that $f(n+e) = f(n)$ for all $n \geq 0$.

We now show how to obtain periodic sequences from eventually periodic ones.

Lemma 3.6. *Let $\{f_1(n)\}, \ldots, \{f_m(n)\}$ be nonzero eventually periodic sequences taking values in a field K and which have distinct indices $a_1, \ldots, a_m$ respectively. Then $\{f_1(n)\}, \ldots, \{f_m(n)\}$ are linearly independent over K.*

Proof. Suppose this is not the case. Then choose m minimal with respect to the property that there exist $f_1, \ldots, f_m$ satisfying the hypotheses of lemma that are linearly dependent over K. By relabelling if necessary, we may assume that $a_1 < \cdots < a_m$. Let L denote the lcm of the minimal periods of $f_1, \ldots, f_m$. Suppose that

$$c_1 f_1(n) + \cdots + c_m f_m(n) \;=\; 0 \qquad \text{for all } n \geq 0.$$

Then

$$c_1 f_1(a_m - 1) + \cdots + c_m f_m(a_m - 1) \;=\; 0,$$

and

$$c_1 f_1(a_m - 1 + L) + \cdots + c_m f_m(a_m - 1 + L) \;=\; 0.$$

Observe that $f_i(a_m - 1) = f_i(a_m - 1 + L)$ for $i < m$ since $f_1, \ldots, f_{m-1}$ all have index at most $a_m - 1$ and have period dividing L. Thus

$$c_m f_m(a_m - 1) = c_m f_m(a_m - 1 + L).$$

But notice, that $f(j + L) = f(j)$ for $j \geq a_m$ and hence $f(a_m - 1 + L) \neq f(a_m - 1)$, or else $\{f(n + a_m - 1)\}$ would be periodic with period dividing L. It follows that $c_m = 0$. But this says that $f_1, \ldots, f_{m-1}$ are linearly dependent. This contradicts the minimality of m. The claim follows. □

Lemma 3.7. *Let $\{f(n)\}$ be an eventually periodic sequence taking values in a field K, and let k be a positive integer. If $\dim_K M_K(f; k) \leq d$, then the index of $\{f(n)\}$ is at most k^d.*

Proof. Let m denote the index of $\{f(n)\}$ and let p denote the minimal period of $\{f(n + m)\}_{n \geq 0}$. We claim that for each $a < \log_m k$, there is some $b < k^a$ such that $\{f(k^a n + b)\}$ has index $\lceil m/k^a \rceil$. To see this, notice that for any $b < k^a$ and $i = \lceil m/k^a \rceil$,

$$\begin{aligned} f(k^a(n + i + p) + b) &= f(k^a n + k^a i + k^a p + b) \\ &= f(k^a n + k^a i + b) \\ &= f(k^a(n + i) + b), \end{aligned}$$

where the penultimate step follows from the fact that $k^a i + b$ is greater than or equal to the index of $\{f(n)\}$. Thus for any $b < k^a$, the index of $\{f(k^a n + b)\}$ is at most $\lceil m/k^a \rceil$. We claim that there exists some $b < k^a$ such that the index of $\{f(k^a n + b)\}$ is at least $\lceil m/k^a \rceil$. If this is not the case then there exist some $i < m/k^a$ such that $f(k^a(n + i + p) + b) = f(k^a(n+i)+b)$ for all $n \geq 0$ and all $b < k^a$. Hence $f(k^a n+b+k^a i+k^a p) = f(k^a n + b + k^a i)$ for all $n \geq 0$. But since this is true for all $b < k^a$ and any integer j has a unique expression as $k^a n + b$, we see that

$$f(j + k^a i + k^a p) \;=\; f(j + k^a i) \qquad \text{for all } j \geq 0.$$

Hence the index of $\{f(n)\}$ is at most $k^a i < m$, a contradiction. Thus for each a there is some $b < k^a$ such that the index of $\{f(k^a n + b)\}$ is exactly $\lceil m/k^a \rceil$. If $k^d < m$, then $\{\lceil m/k^i \rceil \mid 0 \leq i \leq d\}$ has $d+1$ distinct elements. Moreover, there exist $f_0, \ldots, f_d \in M(\{f(n)\}; k)$ such that f_i has index $\lceil m/k^i \rceil$. By Lemma 3.6, these sequences are linearly independent over K, since they are necessarily nonzero. But by assumption $M_K(\{f(n)\}; k)$ has dimension at most d, a contradiction. We conclude that $m \leq k^d$. □

Corollary 3.8. *Let R be a ring, let k be a positive integer, and let $\{f(n)\}$ be an R-valued (R, k)-regular sequence. Suppose that there is a maximal ideal I of R such that:*

- $\{f(n) \bmod I\}$ *is eventually periodic;*
- $M_R(f;k)\otimes_R R/I$ *has dimension at most* d *as an* R/I*-vector space.*

Then $\{f(n+k^d) \bmod I\}$ *is periodic.*

Proof. The result follows easily from Lemma 3.7. □

We now show how to get periods relatively prime to k.

Lemma 3.9. *Let* $\{f_1(n),\ldots,f_d(n)\}$ *be nonzero periodic sequences taking values in some field* K. *Suppose that* f_i *has period* a_i *for* $1 \le i \le d$ *and that* $a_1|a_2|\cdots|a_d$ *and* $a_1,\ldots,a_d$ *are all distinct. Then* $f_1,\ldots,f_d$ *are linearly independent over* K.

Proof. Suppose not. Then we can choose d minimal with respect to the property that there exist such $f_1,\ldots,f_d$ that are linearly dependent. Then there exist integers $c_1,\ldots,c_d$ such that

$$c_1f_1(n)+\cdots+c_df_d(n) \;=\; 0 \qquad \text{for all } n\ge 0.$$

Notice that $f_i(n+a_{d-1}) = f_i(n)$ for $i<d$. Thus

$$c_1f_1(n)+\cdots+c_{d-1}f_{d-1}(n)+c_df_d(n+a_{d-1}) \;=\; 0.$$

Subtracting we see that $c_d\big(f_d(n+a_{d-1})-f_d(n)\big)=0$ for all n. Since f_d has period $a_d>a_{d-1}$, we conclude that $c_d=0$. But this contradicts the minimality of d. The result now follows. □

Proposition 3.10. *Let* $\{f(n)\}$ *be a periodic sequence taking values in a field* K *and let* k *be a positive integer. If* $\dim_K M_K(f;k)\le d$ *then for* $0\le j<k^d$, *the sequence* $\{f(k^dn+j)\}$ *is periodic with minimal period relatively prime to* k.

Proof. Let e denote the minimal period of $\{f(n)\}$. Suppose that the period of $f(k^dn+j)$ is not relatively prime to k. Then the sequence is necessarily nonzero. Pick $0=j_0,j_1,\ldots,j_d=j$ with the property that $0\le j_i<k^i$ and $j\equiv j_i \bmod k^i$. We claim that the (nonzero) sequences

$$\{\{f(k^in+j_i)\}\mid 0\le i\le d\}$$

are linearly independent over K. Let q_i denote the minimal period of the sequence $\{f(k^in+j_i)\}$. Observe that q_{i+1} divides $q_i/\gcd(k,q_i)$. Moreover, by assumption $\{f(k^dn+j_d)\}$ does not have minimal period relatively prime to k and thus $q_0,q_1,\ldots,q_d$ must all have some factor in common with k. Hence

$$q_d \;<\; q_{d-1} \;<\; \cdots \;<\; q_0.$$

Thus by Lemma 3.9, we see that the sequences

$$\{\{f(k^in+j_i)\}\mid 0\le i\le d\}$$

are linearly independent over K. But $M(\{f(n)\}; k)$ has dimension at most d and so we get an immediate contradiction. $\square$

We are now ready to give our most important result about rational k-regular sequences.

Theorem 3.11. *Let R be a finitely generated integral domain over $\mathbb{Z}$, let k be a positive integer, and let $\{f(n)\}$ be a (R, k)-regular sequence taking values in R. Then $\{f(n)\}$ satisfies a linear recurrence over R if and only if $\{f(n) \bmod I\}$ is eventually periodic for infinitely many maximal ideals I whose intersection is (0).*

Proof. Suppose that $\{f(n)\}$ satisfies a linear recurrence over R and let I be a maximal ideal in R. Then $\{f(n) \bmod I\}$ takes values in R/I, which is a finite field by Corollary 2.3. It follows that $\{f(n) \bmod I\}$ is eventually periodic for every maximal ideal I (see Everest et al. [14, pp. 45-46]).

Conversely, suppose that $\{f(n)\}$ is eventually periodic mod I for infinitely many maximal ideals I whose intersection is (0) and let $\mathcal{M}$ denote the set of such ideals. Let d be the size of a minimial generating set for $M(\{f(n)\}; k)$ as an R-module. We define $g(n) = f(n + k^d)$ for $n \geq 0$. We note that $\{g(n)\}$ is an (R, k)-regular sequence. By Corollary 3.8, $\{g(n) \bmod I\}$ is periodic for each maximal ideal I in $\mathcal{M}$. By Proposition 3.10, for $0 \leq j < k^d$ we have that $g_j(n) := g(k^d n + j)$ is periodic mod I with period relatively prime to k for each maximal ideal I in $\mathcal{M}$. Hence $\{g_j(n)\}$ satisfies a linear recurrence for $0 \leq j < k^d$ by Theorem 3.4. By Lemma 3.1, we see that $\{g(n)\}$ satisfies a linear recurrence and so $\{f(n)\}$ satisfies a linear recurrence, again by Lemma 3.1. $\square$

4. Reduction to finitely generated integral domains

Proposition 4.1. *Let R be a commutative ring, let k be a positive integer, and let f be an (R, k)-regular sequence taking values in an R-module A. Then f is (S, k)-regular for some finitely generated $\mathbb{Z}$-subalgebra S of R. Furthermore there is some finitely generated S-submodule B of A such that f takes values in B.*

Proof. Since $\{f(n)\}$ is (R, k)-regular, there exist a positive integer d, R-valued $d \times d$ matrices $X_0, \ldots, X_{k-1}$, and sequences $\{a_i(n)\}$, $1 \leq i \leq d$ such that if

$$\mathbf{v}(n) \;=\; \begin{bmatrix} a_1(n) \\ a_2(n) \\ \vdots \\ a_d(n) \end{bmatrix}$$

then $\mathbf{v}(kn+j) = X_j\mathbf{v}(n)$ for $0 \le j < k$ (cf. Allouche and Shallit [3, Theorem 16.1.3]).

Let S be the $\mathbb{Z}$-subalgebra of R generated by the entries in $X_0, \ldots, X_{k-1}$ and let B be the S-submodule of A spanned by the entries in $\mathbf{v}(0)$. Then by construction $\{f(n)\}$ is (S,k)-regular and takes values in B (cf. Allouche and Shallit [3, Theorem 16.1.3]). □

We note that this interpretation of regular sequences in terms of monoid homomorphisms from $\{0,1,2,\ldots,k-1\}^*$ to $M_d(R)$ is closely related to *recognizable series* [5].

Lemma 4.2. *Let R be a commutative ring, let k be a positive integer, and let $\{f(n)\}$ be an (R,k)-regular sequence taking values in a principle ideal Ra of R. If $\{g(n)\}$ is an R-valued sequence satisfying $f(n) = ag(n)$ for all $n \ge 0$, then $\{g(n) \bmod J\}$ is R/J regular, where J is the annihilator of a.*

Proof. Pick a finite set of generators $\{f_1, \ldots, f_d\}$ for $M(f;k)$. For each i, there is some function g_i in $M(g;k)$, corresponding to f_i, with the property that $f_i = ag_i$. We claim that $\{g_1(n) \bmod J, \ldots, g_d(n) \bmod J\}$ spans $M_{R/J}(\{g(n) \bmod J\};k)$ as an R/J-module. To see this, suppose that $h(n) \in M(g;k)$ has the property that $h(n) \bmod J$ is not in the span of this set. We have $ah(n) \in M(f;k)$, and hence there exist $r_1, \ldots r_d \in R$ such that

$$ah = \sum_{i=1}^{d} r_i f_i.$$

Equivalently,

$$ah = \sum_{i=1}^{d} ar_i g_i.$$

Thus $h(n) - \sum r_i g_i(n)$ annihilates a for all n. Consequently,

$$h \equiv \sum_{i=1}^{d} r_i g_i \bmod J,$$

a contradiction. □

Proof of Theorem 1.4. The proof of this result uses a series of reductions.

First Reduction: We may assume that R is finitely generated as a $\mathbb{Z}$-algebra and $f(n)$ takes values in a finitely generated R-module.

By Proposition 4.1, we see that $\{f(n)\}$ is (S,k)- and (S,ℓ)-regular for some finitely generated $\mathbb{Z}$-subalgebra of R; moreover, $\{f(n\}$ takes values in some finitely generated S-module A. Since a linear recurrence over S is also a linear recurrence over R, it is no loss of generality to assume that R is a finitely generated $\mathbb{Z}$-algebra and that $\{f(n)\}$ takes values in a finitely generated R-module A.

Second Reduction: We may assume that the $\{f(n) \bmod J\}$ satisfies a linear recurrence over R/J for every nonzero ideal J.

We may assume that $f(n)$ does not satisfy a linear recurrence over R. Since R is finitely generated over $\mathbb{Z}$, it is Noetherian. Thus we can pick an ideal I maximal with respect to the property that there exists a sequence which is both $(R/I, k)$- and $(R/I, \ell)$-regular and yet does not satisfy a linear recurrence. Replace R with R/I and pick a sequence $\{f(n)\}$ which is both (R, k)- and (R, ℓ)-regular and yet does not satisfy a linear recurrence over R. Then $\{f(n) \bmod J\}$ satisfies a linear recurrence over R/J for every nonzero ideal J in R.

Third Reduction: We may assume that R is an integral domain.

Suppose that this is not the case. Then there is a nonzero element a whose annihilator J is nonzero. By assumption, $f(n) \bmod aR$ satisfies a linear recurrence and hence there exist $c_1, \ldots, c_m \in R$ such that

$$f(n) \ = \ \sum_{i-1}^{m} c_i f(n-i) \bmod aR.$$

Let $g(n) = f(n) - \sum c_i f(n-i)$. Then $\{g(n)\}$ is (R, k)-regular and (R, ℓ)-regular and takes values in aR. Pick an R-valued sequence $\{h(n)\}$ satisfying $g(n) = ah(n)$ for all $n \geq 0$. By Lemma 4.2, $h(n) \bmod J$ is $(R/J, k)$- and $(R/J, \ell)$-regular and hence satisfies a linear recurrence over R/J; that is, there exist $d > 0$ and $r_1, \ldots, r_d \in R$ such that

$$h(n) \ \equiv \ \sum_{i=1}^{d} r_i h(n-i) \bmod J \qquad \text{for } n \geq d.$$

Multiplying both sides by a gives

$$g(n) \ = \ \sum_{i=1}^{d} r_i g(n-i),$$

and so $\{g(n)\}$ satisfies a linear recurrence over R. This immediately gives a linear recurrence satisfied by $\{f(n)\}$ over R. Thus it is no loss of generality to assume that R is an integral domain.

Fourth Reduction: We may assume that $\{f(n)\}$ is R-valued.

We already may assume that $\{f(n)\}$ takes values in a finitely generated R-module A. Since A is Noetherian, we can pick a submodule B of A maximal with respect to the property that $\{f(n) + B\}$ does not satisfy a recurrence over R. Replacing A with A/B, we can assume that $\{f(n) +$

$A'\}$ satisfies a recurrence over R for all nonzero submodules A' of A. Pick a nonzero $a \in A$ and consider the short exact sequence

$$0 \;\to\; Ra \;\to\; A \;\to\; A/Ra.$$

Notice that the reduced sequence $\{f(n) + Ra\}$ satisfies a recurrence over R. Let $g(n)$ be a sequence satisfying a linear recurrence over R which takes values in A such that $g(n) - f(n) \in Ra$ for all $n \geq 0$. (Note that this can be done simply by "pulling back" the initial values of $\{f(n) + Ra\}$ in A/Ra to initial values in A and then declaring that $g(n)$ satisfies the same recurrence as the one satisfied by $\{f(n) + Ra\}$.) Notice $h(n) := f(n) - g(n)$ cannot satisfy a linear recurrence over R as $f(n)$ does not; moreover, it takes values in the module Ra. This module is isomorphic to $R/\mathrm{Ann}(a)$. Observe that $h(n)$ can be regarded as an $(R/\mathrm{Ann}(a), k)$- and $(R/\mathrm{Ann}(a), \ell)$-regular sequence and thus if $\mathrm{Ann}(a)$ is nonzero, then it satisfies a linear recurrence over $R/\mathrm{Ann}(a)$ by our choice of R. Moreover, this linear recurrence lifts to a linear recurrence over R by the fact that $h(n)$ takes values in a module that is annihilated by $\mathrm{Ann}(a)$. Thus $\mathrm{Ann}(a) = 0$. Replacing, $f(n)$ by $h(n)$, we may assume that $f(n)$ is R-valued.

And so we may assume that $f(n)$ is an (R, k)- and (R, ℓ)-regular sequence taking values in R and R is a finitely generated domain over $\mathbb{Z}$. Since R is a finitely generated domain over $\mathbb{Z}$, we have that R/I is finite dimensional for each maximal ideal I of R and the intersection of all maximal ideals is (0) by Corollary 2.3. Hence $\{f(n) \bmod I\}$ is both k- and ℓ-automatic for every maximal ideal I. It follows from Cobham's theorem that $\{f(n) \bmod I\}$ is eventually periodic for every maximal ideal I. Since the intersection of all maximal ideals is (0), we see that $\{f(n)\}$ satisfies a linear recurrence over R by Theorem 3.11. The result follows. $\square$

Proof of Theorem 1.5. Suppose first that $\{f(n)\}$ is k- and ℓ-regular. By Theorem 1.4

$$\mathbf{F}(x) \;:=\; \sum_{n=0}^{\infty} f(n)x^n \;\in\; \mathbb{Z}[[x]]$$

is the power series expansion of a rational function $p(x)/q(x)$ with $p, q \in \mathbb{Z}[x]$ and $q(0) = 1$. Note that $f(n) = \mathrm{O}(n^d)$ for some positive integer d (see Allouche and Shallit [3, Theorem 16.3.1]). Hence $\mathbf{F}(x)$ has no poles inside the unit circle and so $q(x)$ must have leading coefficient ± 1. Since $q(0) = 1$, we conclude that $\mathbf{F}(x)$ has all of its poles on the unit circle. Since $q(x)$ has integer coefficients, these poles must all be roots of unity. Conversely, Allouche and Shallit [3, Theorem 16.4.2] show that the power series expansion of a rational function having all its poles at roots of unity is k-regular for all $k \geq 1$. $\square$

5. Concluding remarks

We note that Theorem 1.5 appears as a conjecture in Allouche and Shallit [3, §16.8, item 16.3]. In this form, it is a special case of a conjecture due to van der Poorten. Given a power series

$$\mathbf{F}(x) \ = \ \sum_{n=0}^{\infty} f(n)x^n \ \in \ \mathbb{Z}[[x]],$$

we say that $\mathbf{F}(x)$ is *k-Mahler* if $\mathbf{F}(x)$ satisfies a functional equation of the form

$$F(x^{k^m}) \ = \ \sum_{i=0}^{m-1} p_i(x)\mathbf{F}(x^{k^i}). \tag{5.1}$$

k-regular sequences are a special subset of the set of k-Mahler sequences.

Conjecture 5.1 (van der Poorten [22])**.** *Let $\mathbf{F}(x)$ be a power series which is both k- and ℓ-Mahler. If k and ℓ are multiplicatively independent then $\mathbf{F}(x)$ is the power series expansion of a rational function.*

Some work has been done on this by various authors [23], [24], [10], [4]. In fact, van der Poorten [22] outlined a proof of the conjecture, but the proof is incomplete.

6. Acknowledgments

I thank Jean-Paul Allouche, Jeff Shallit, and Harm Derksen for many helpful comments and discussions.

References

[1] J.-P. Allouche and J. Shallit. The ring of k-regular sequences. *Theoret. Comput. Sci.* **98** (1992), 163–197.
[2] J.-P. Allouche and J. Shallit. The ring of k-regular sequences, II. *Theoret. Comput. Sci.* **307** (2003), 3–29.
[3] J.-P. Allouche and J. Shallit. *Automatic sequences. Theory, applications, generalizations.* Cambridge University Press, Cambridge, 2003.
[4] P.-G. Becker. k-Regular power series and Mahler-type functional equations. *J. Number Theory* **49** (1994), 269–286.
[5] J. Berstel and C. Reutenauer. *Rational Series and Their Languages* EATCS Monographs on Theoretical Computer Science (12), W. Brauer, G. Rozenberg, A. Salomaa (Eds.) Springer-Verlag Berlin, Heidelberg 1988.
[6] A. Cobham. On the base-dependence of sets of numbers recognizable by finite automata. *Math. Systems Theory* **3** (1969), 186–192.
[7] M. Dekking, M. Mendès France, and A. van der Poorten. Folds. *Math. Intelligencer* **4** (1982), no. 3, 130–138. Erratum: **5** (1983), 5.
[8] M. Dekking, M. Mendès France, and A. van der Poorten. Folds. II. Symmetry disturbed. *Math. Intelligencer* **4** (1982), no. 4, 173–181. Erratum: **5** (1983), 5.

[9] M. Dekking, M. Mendès France, and A. van der Poorten. Folds. III. More morphisms. *Math. Intelligencer* **4** (1982), no. 4, 190–195. Erratum: **5** (1983), 5.

[10] P. Dumas. Algebraic aspects of B-regular series. In A. Lingas, R. Karlsson, A. Carlsson, editors, *Proc. 20th Int. Conf. on Automata, Languages, and Programming*, Vol. 700 of *Lecture Notes in Computer Science,* 457–468. Springer-Verlag, 1993.

[11] F. Durand. A generalization of Cobham's theorem. *Theory Comput. Systems* **31** (1998), 169–185.

[12] F. Durand. A characterization of substitutive sequences using return words. *Discrete Math.* **179** (1998), 89–101.

[13] D. Eisenbud. *Commutative algebra. With a view toward algebraic geometry.* Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995.

[14] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward. *Recurrence sequences.* Mathematical Surveys and Monographs, 104. American Mathematical Society, Providence, RI, 2003.

[15] S. Fabre. Une généralisation du théorème de Cobham. *Acta Arith.* **67** (1994), 197–208.

[16] I. Fagnot. On the subword equivalence problem for morphic words. *Discrete Appl. Math.* **75** (1997), no. 3, 231–253.

[17] G. Hansel and T. Safer. Vers un théorème de Cobham pour les entiers de Gauss. *Bull. Belg. Math. Soc. Simon Stevin* **10** (2003), 723–735.

[18] G. Hansel. À propos d'un théorème de Cobham. In D. Perrin, editor, *Actes de la Fête des Mots,* 55–59. Greco de Programmation, CRNS, Rouen, 1982.

[19] G. Hansel. Systèmes de numération indépendants et syndéticité. *Theoret. Comput. Sci.* **204** (1998), 119–130.

[20] K. Nishioka. Mahler functions and trancendence. *Lecture Notes in Mathematics* **1631**. Springer-Verlag, Berlin, 1996.

[21] F. Point and V. Bruyère. On the Cobham-Semenov theorem. *Theory Comput. Systems* **30** (1997), 197–220.

[22] A. J. van der Poorten. Remarks on Roth's theorem. *Séminaire de Théorie des Nombres, Paris* 1986–87, 443–452, Progr. Math., **75**, *Birkhäuser Boston, Boston, MA*, 1988.

[23] B. Randé. Récurrences 2- et 3-mahlériennes. *J. Théor. Nombres Bordeaux* **5** (1993) 101–109.

[24] B. Randé. Équations fonctionnelles de Mahler et applications aux suites p-régulières. PhD thesis, Université Bordeaux I, 1992.